WIZ

In association with CSO

Why disruptive technology is needed to protect from cloud era threats

Building faster and more securely in the cloud requires unified visibility, innovative approaches, and new thinking

Table of contents

Introduction

Organizations are adopting cloud technologies faster than they can secure them against emerging cybersecurity threats.

Often understaffed security teams are reacting to a seemingly never-ending stream of alerts that impede their ability to anticipate and address very real risk signals hidden within the "noise." They're reliant on disparate, domain-specific security tools that lack context. They are weighed down by the time required to operationalize new security tools. And cloud providers and customers lack the shared responsibility needed to quickly nullify newly discovered threats.

IT leaders need to adopt a more proactive approach. Organizations can't afford to be continuously reacting to the latest threats. They need a new strategy that's both frictionless to deploy and provides complete visibility into an increasingly complex environment so they can protect their businesses.

This Tech Dossier examines the limitations of security strategies that project risk-prone tactics into new cloud environments, provides practical advice on embedding a shift-left security approach within an organization and highlights a new cloud-native security approach that moves teams into the proactive posture needed to remove risks before they become threats.

1 | New security challenges today and tomorrow

Companies increasingly are deploying applications and services across multiple clouds and relying on multiple application architectures. That is a challenge for any security team, especially those with resource constraints.

Organizations are increasingly embracing multicloud environments. According to one survey, 56% of enterprises with more than 5,000 employees have already adopted multicloud and 80% plan to do so within 1-3 years.

The speed of adoption, however, is outpacing the ability to protect an ever-changing environment that spans on-premises, private clouds, and multiple public clouds. Developers are racing to implement new cloud applications and services but doing so independently of security teams. This is creating a widening gap between how the cloud is used and how it should be used securely.

There is broad lack of visibility among most organizations into the totality of their cloud assets, who is using these assets, or whether they are vulnerable. According to the Wiz 2022 cloud security threats report, more than 55% of companies have at-least one database that is currently publicly exposed to the internet and 70% of cloud resources are not protected by any endpoint protection product.

Today, many organizations are grappling with lack of visibility into their software supply chain. The SolarWinds compromise, for example, was distributed as part of a normal platform update, putting at risk both cloud and on-premises environments.

Some risks are introduced by adoption of open source code, such as the remote code execution vulnerability known as Apache Log4Shell that is embedded in many Java applications and web services. Others result from granting 3rd party vendors permissions within an enterprise's cloud environment. An analysis of 1,500 AWS accounts found that 76% granted vendor permissions that would enable full control over a customer's cloud, risking account takeover attacks.

When organizations rely on cloud providers, they are potentially at risk from flaws in code, packages, and default configurations in the provider's infrastructure. The U.S. Cybersecurity and Infrastructure Security Agency (CISA) maintained a Known Exploited Vulnerabilities (KEV) catalog which lists more than 350

More than

55%

of companies have at-least one database that is currently publicly exposed to the internet

70%

of cloud resources are not protected by any endpoint protection product.

56% **of enterprises with more than 5,000 employees have already adopted multicloud**

80% **plan to do so within 1-3 years**

vulnerabilities for agencies to detect and mediate, but that represents less than 1% of vulnerabilities detected in the cloud.

Lack of visibility into these threats slows the ability of organizations to bring new services and products to market or causes them to violate compliance requirements.

2 | Agent-based approach lacks agility, flexibility

Most enterprise security strategies rely heavily on software-based security agents. These agents are employed by multiple systems for vulnerability scanning, threat detection, data loss prevention (DLP), remote management, virtual private networks (VPN), and more.

Only
20%
of virtual machines (VMs) had endpoint protection agents, even though they often have identity and network access to critical infrastructure.

Most of these agents are good for what they were designed for, but they reflect a legacy mindset in which domain-specific tools protected different parts of the on-premises infrastructure. They lack context into the complexities of multi-environment, multi-workload, and multi-project cloud estates, and are unable to correlate the activities within their specific domain and what is happening across the full environment.

Managing, deploying, and updating countless endpoint agents is a no-win strategy, especially as enterprises deploy more Internet of Things (IoT) and edge devices, some of which may be intermittently connected. In the cloud, it's even more complex since IT teams do not necessarily have control over all the deployed workloads.

An organization dependent on these agents is at risk from lack of coverage, deployment difficulties, an increased attack surface, potential for exploitation of high privileges, and ease of avoidance by attackers.

Cloud resources are mostly managed by DevOps teams, which usually prioritize performance and operability. Security is often sidelined, or an afterthought in the development process, creating a fundamental challenge.

Research by Wiz found that only 20% of virtual machines (VMs) had endpoint protection agents, even though they often have identity and network access to critical infrastructure. This creates a severe blind spot in environments that rely exclusively on agent-based solutions.

Security agents must be granted high privileges in the operating system to prevent or detect threats. Thus, they represent a tempting target for malicious attackers seeking to exploit local privilege escalation (LPE) vulnerabilities.

When attackers gain access to a VM, one of the first things they check are all the running processes and services, and specifically which security agents are present. After identifying the security agents, attackers can better plan their next steps based on their knowledge of how the agent operates. Attackers may also scan for

With growing reliance on clouds, it's time to move beyond the agent-bound legacy mindset to a new agentless security approach designed to accommodate the emerging multi-cloud model.

credentials such as hard coded secrets improperly stored within their cloud services that if discovered may provide access to confidential information or to other systems. This information can also provide lateral movement paths using identity vs network.

With growing reliance on clouds, it's time to move beyond the agent-bound legacy mindset to a new agentless security approach designed to accommodate the emerging multi-cloud model. Agentless scanning can build an inventory of cloud infrastructure across workloads, accounts, and environments. That will enable organizations to correlate risk signals across the multi-cloud environment and enable comprehensive risk assessment of the entire security stack.

3 | Cloud has disrupted everything but security strategies

Cloud estates represent a complex interconnection of technologies, architectures, and environments. The cloud era demands a cloud-based security strategy.

Today's IT infrastructure encompasses VMs, containers, platform-as-a-service, operating systems, coding languages, frameworks, and much more. Separate, autonomous teams typically manage different parts of these interconnected assets based on how they managed on-premise environments in the past.

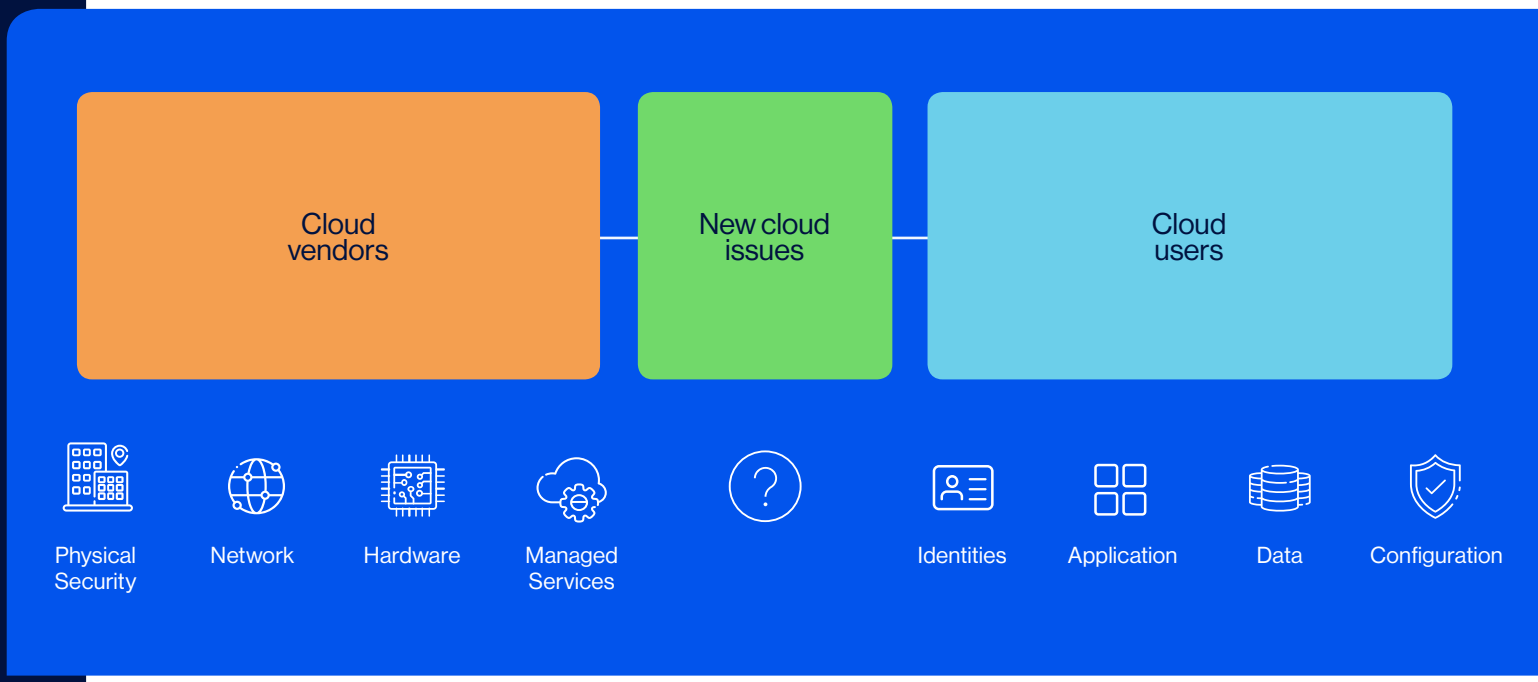
Siloed teams primarily rely on their own sets of tools, resulting in a fragmented view of risk. It is unrealistic to expect that they can manually correlate the thousands of alerts typically generated daily.

Many enterprises are speeding up the deployment and updating of software by breaking down silos that segmented software development and IT operations and instead creating integrated DevOps processes. That ensures that operations are not an afterthought of the development process, which frequently resulted in inefficiencies and failed projects.

Building on the success of DevOps, forward-thinking organizations have attempted to "shift-left" security into the development process—known as DevSecOps.

Building on the success of DevOps, forward-thinking organizations have attempted to "shift-left" security into the development process—known as DevSecOps. Fixing vulnerabilities and misconfigurations in the pipeline before deployment makes perfect sense - it reduces the overall threat footprint and saves time.

The promise of "shifting left" has proven much harder than expected. It is challenging to efficiently operationalize and many security teams struggle to enforce policies without creating friction. Security tooling is often fragmented from development to runtime, making it impossible to build efficient, predictable, and secure workflows.



For the most part, security tooling reflects the on-premise, point solution mode of the pre-cloud IT environment. Largely siloed, security teams are not well-equipped to deal with the challenges of cloud environments that have no silos. Even new cloud-oriented security solutions are primarily a mix-and-match of acquired technologies that run independently with little or no correlation.

Security is further hindered by the inability of enterprises and cloud vendors to consistently adhere to a shared security model. Although cloud services providers rightly boast of their ability to employ well-tooled security teams, customers are not absolved of their responsibility to actively manage security.

Cloud Service Providers (CSPs) are responsible for their own infrastructure, such as security of the cloud. If vulnerabilities are found on the CSP itself, these are often fixed without customer input before the issue is made public. Meanwhile customers are responsible for their own workloads/services, and ultimately, their data in the cloud. This can become a grey area since the demarcation point of responsibility moves depending on the type of cloud service varying between infrastructure as a service (IaaS), function as a service (FaaS), and platform as a service (PaaS).

These issues equally apply to software vendors, operating system vendors and open source projects. Providers typically distribute frequent advisories of actions that customers need to take to deal with newly discovered vulnerabilities. Customers that don't manually implement those actions are left exposed. Notifications can sometimes be worded vaguely so customers don't realize they specifically are impacted, and it can be difficult to track and prioritize vulnerabilities, and other associated flaws, across the full, diverse stack of technologies they are using within the cloud.

Wiz's unique architecture allows for seamless scanning of the entire cloud environment across all compute types and cloud services for vulnerabilities, configuration, network, and identity issues without agents or sidecars.

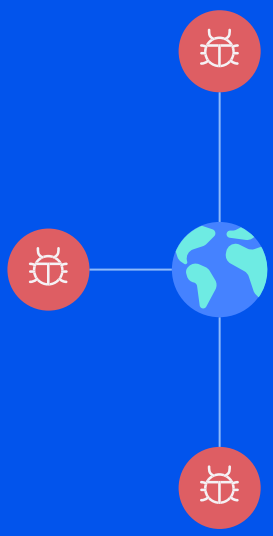
4 | Disrupting established cybersecurity models

A new, cloud-native cybersecurity approach from Wiz addresses the inherent weaknesses in agent-based security solutions and the problems of the shared responsibility model. Wiz's unique architecture allows for seamless scanning of the entire cloud environment across all compute types and cloud services for vulnerabilities, configuration, network, and identity issues without agents or sidecars.

The Wiz solution builds an inventory of a customer's cloud infrastructure across workloads, accounts, users, and environments. This disruptive approach to security provides customers with a single, unified policy framework that delivers end-to-end visibility across the entire stack and correlates interconnected risk factors. The full technology stack, including VM images, container images and serverless functions , is monitored for compliance violations across dozens of industry standards.

The solution continuously analyses configurations, vulnerabilities, network, identities, access, and exposed secrets across accounts, users, and workloads. Applying security on the right first, gives organisations full visibility, which then facilitates the journey to begin shifting left. Wiz allows organisations to shift left using the same sets of policies and controls using a unified rulebase. Fixing vulnerabilities and misconfigurations in the pipeline before deployment reduces the overall threat footprint and saves time.

Wiz determines the end-to-end network path for VMs, containers, and serverless functions by calculating their true effective exposure for every cloud object, based on analyses of security groups, firewall rules, routing tables and other factors.



Threats discovered by Wiz researchers

A team of Wiz security researchers tasked with finding new attack surfaces in the cloud has uncovered significant vulnerabilities. One of those, dubbed ChaosDB, potentially could provide complete unrestricted access to the databases of several thousand Microsoft Azure customers.

Another vulnerability, named OMIGOD, involves a software agent called Open Management Infrastructure (OMI) embedded in many Azure services that could allow attackers to escalate to root privileges and remotely execute malicious code.

On AWS, the research team discovered three cross-account vulnerabilities in different AWS services that allow anyone to read or write into the accounts of other AWS customers. Wiz research also revealed high numbers of organizations granting high privileges unknowingly to 3rd party vendors on AWS.

The Wiz research team also discovered a new class of vulnerabilities that expose dynamic DNS data traffic from millions of endpoints. The Wiz research team is constantly testing for additional vulnerabilities that expose organizations to new threats.

Wiz works with the leading cloud providers to help their customers remove the most pressing risks in the cloud environments. That includes Amazon Web Services, Google Cloud, Microsoft Azure, and Oracle Cloud, as well as container services such as Kubernetes and Fargate..

A 100% API-based approach provides rapid speed of deployment, connecting across the technology stack within minutes. Wiz scales to any cloud environment with zero impact on resource or workload performance, greatly improving security, and availability—without slowing down developers or business operations.

Wiz helps organizations rapidly remove the most critical risks in their cloud environments, exposing toxic combinations across the security stack and providing the ability to proactively remove risks and prevent risks from becoming breaches. With its disruptive technology, organizations can transform security into a technology enabler, rather than a technology blocker.

5 | What's different about Wiz

Wiz was founded in January 2020 by the former leads of Microsoft's Cloud Security Group, who were also the founding team of Adallom, the fast-growing cloud access broker security (CASB) that was acquired by Microsoft in 2015. It was sparked with the ambitious objective to completely change how the industry approaches cloud security.

The Wiz solution is built from the ground up to align to customized enterprise workflows. It embraces and works through the complexity of cloud to automate the identification of real attack vectors, maximizes security ROI, and is easy to implement and operationalize across security, DevOps, and development teams.

Wiz offers dozens of out-of-the-box integrations for common SIEM, SOAR, ticketing, and messaging tools. It also integrates with CI/CD tools like Github Actions , Jenkins or Azure DevOps , and offers a fully extensible API for unlimited workflow customizations.

Wiz secures organizations that build and run in the cloud. Founded in 2020, the company is the fastest-growing software-as-a-service provider in the world, reaching a $6 billion valuation in less than two years.

Wiz enables hundreds of organizations, including more than 20 percent of the Fortune 500, to rapidly identify and remove critical risks in cloud environments so they can build faster and more securely. Its customers include Salesforce, Mars, Fox, BMW, Slack, Aon, Cushman & Wakefield, DocuSign, MassMutual, Agoda and UiPath, among others.

Wiz is backed by Sequoia, Index Ventures, Insight Partners, Salesforce, Blackstone, Advent, Greenoaks and Aglaé. Visit https://www.wiz.io/ for more information.

Download the full 2022 Cloud Security Threats Report

Download